11-01-02

#2 11-20-02 92002

28-78

OIPE
OCT 31 2002
TC 1100
PATENT & TRADEMARK OFFICE

DOCKET: 4135-4000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Robert Gagnon et al.	**Group Art Unit:** TBA
Serial No.	:	09/772,132	**Examiner:** TBA
Filing Date	:	January 29, 2001	
For	:	SYSTEM AND METHOD FOR WIRELESS ACCESS TO A USER'S COMPUTER	

RECEIVED
NOV 13 2002
Technology Center 2100

Commissioner For Patents
Washington, D.C. 20231
BOX PETITION

PETITION TO MAKE SPECIAL UNDER 37 C.F.R. §1.102(d) (XI)

Sir :

This is a Petition to Make Special the above-identified patent application. The basis for this Petition is that the above-referenced application is an invention for countering Terrorism. Enclosed is the appropriate Petition fee under 37 C.F.R. 1.17(h).

The ability of law enforcement and intelligence officials to timely communicate over a secure cellular network in times of crisis is critical, such as in a terrorist attack. The accessibility of emergency communications in a cellular networks during events such as a terrorist attack is problematic. For current wireless devices to access computer and databases, such as a government search engine, the current wireless devices require significant processing and memory capacities, such as devices located in police vehicles.

This patent application allows law enforcement and intelligence officials to timely and securely communicate in times of crisis, such as in a terrorist attack, over any cellular network using any type of wireless device. The user is able to access a database regardless of the device's language, or protocol used. The user's device is allowed to communicate to computers and

11/04/2002 AWONDAF1 00000032 09772132
01 FC:1460 130.00 OP

databases such as a terrorist watch list. The invention allows users to have instant access to law enforcement and intelligence information. For example, the applicant's invention allows field personal to have access to searches of criminal records, license plates, driving records, and social security numbers. The invention can also be enabled to provide critical and timely access to the databases of F.B.I., C.I.A., INTERPOL, and other law enforcement and intelligence databases. All this information is available to law enforcement personnel on any wireless device such as a cell phone or personal digital assistant (PDA) like a Palm™ handhelds. Enclosed are documentation from the Applicant's website to further support this Petition.

In view of the above, Applicant respectfully requests that this Petition to Make Special be granted. It is believed that a fee is due for the filing of this Petition in accordance with 37 C.F.R. 1.17(h). A check in the amount of $130.00 is enclosed with this Petition. However, any additional fees which are necessitated for the proper consideration of this paper may be charged to Deposit Account No. 13-4500 (Order No. 4135-4000). A duplicate copy of this document is enclosed for this purpose.

Respectfully submitted,

Dated: Oct. 31, 2002

MORGAN & FINNEGAN

By: _____

Keith J. McWha
Attorney for the Applicants
Reg. No. 44,235

MORGAN & FINNEGAN
345 Park Avenue
New York, New York 10154
212-758-4800 Telephone
212-751-6849 Facsimile

databases such as a terrorist watch list. The invention allows users to have instant access to law enforcement and intelligence information. For example, the applicant's invention allows field personal to have access to searches of criminal records, license plates, driving records, and social security numbers. The invention can also be enabled to provide critical and timely access to the databases of F.B.I., C.I.A., INTERPOL, and other law enforcement and intelligence databases. All this information is available to law enforcement personnel on any wireless device such as a cell phone or personal digital assistant (PDA) like a Palm™ handhelds. Enclosed are documentation from the Applicant's website to further support this Petition.

In view of the above, Applicant respectfully requests that this Petition to Make Special be granted. It is believed that a fee is due for the filing of this Petition in accordance with 37 C.F.R. 1.17(h). A check in the amount of $130.00 is enclosed with this Petition. However, any additional fees which are necessitated for the proper consideration of this paper may be charged to Deposit Account No. 13-4500 (Order No. 4135-4000). A duplicate copy of this document is enclosed for this purpose.

Respectfully submitted,

Dated: Oct. 31, 2002

MORGAN & FINNEGAN

By: _____

Keith J. McWha
Attorney for the Applicants
Reg. No. 44,235

MORGAN & FINNEGAN
345 Park Avenue
New York, New York 10154
212-758-4800 Telephone
212-751-6849 Facsimile

PoliceMobility.com

May 9, 2002

Welcome to PoliceMobility, a specialty area of Penokio Technology for Law Enforcement and Intelligence Service use. This site is password protected and certain sections are off limits for r industry visitors.

Penokio.com is a PAT Pending Technology that permits wireless two-way control of existing la enforcement and Intelligence application from any wireless device. The cost savings from exist application retrofit ensures that organizations are not prevented by cost of entry. Our products administrators to focus human resources on Prevention and Investigation and not pushing pap

FroZen Dirt Media's NCAGE (NATO Commercial and Government Entity) number is L0622

Certain Information is only available on client site.

©Copyright 2002 FroZen Dirt Media Corp. All Rights Reserved.

Penokio: Couloir

SYLLABICATION: cou·loir
PRONUNCIATION: kōōl-wär'
NOUN: A deep mountainside gorge or gully, especially in the Swiss Alps.
ETYMOLOGY: French, from *couler*, to slide, to flow. See coulee.

Introduction:

This document is a low level technical and operational discussion paper introducing the Penokio technology and it's possible contribution to HUMINT gathering and communication. The MIL/INTEL uses of the technology have been non-public and known only to key personnel. This technology is currently PAT PENDING but can be suppressed for National Security reasons.

Cell Phone Ubiquity as natural cover

By 2005 the cellular industry estimates over 1.5 Billion cellular phones in use worldwide and that over 85% will be data enabled (access to internet). The Intel collection and communication possibilities are revolutionary.

Most intelligence related "tools" are recognizable as such and subsequently can be used to identify operatives and negate the operation. The more unique or special a thing, the fewer people will have it. Unique tools may also have unique needs (line of sight, power, antennae, assembly) or have unique signatures (hard to disguise or cover up). Technologically speaking, the more ubiquitous a device the harder to single out users for scrutiny and the easier for the user to obtain replacements or operate in the open.

Cellular Web devices are able to provide a necessary link to important data and more importantly provide a reasonably secure method of inputting data in the field.

Data Input and Response

Intelligence to be effective must be timely. Operatives ideally will have on demand access to resources and able to input new data that others can have instant access to. Penokio: Couloir can provide input/query access for field personnel to perform basic functions such as :

- License Plate rundown
- Criminal record search
- DL information
- Social Security Information

Penokio: Couloir can also provide access and direct input to sources such as:

- CPIC- Canadian Police Information Centre
- CIA- To be determined (Watch list, RFI, Telemetry)
- NSA- As Above
- FBI- Manhunt info, Records, Intel
- INTERPOL- Police records, Intel
- RCMP- Police Records, Intel
- Oversight- Aggregate for hand sort

Access control

Cellular devices are simplistic in their approach to security but sufficient for protection from most forms of interception. The devices currently have the ability to use 32bit encryption (low level) but this will be improved to 64bit in the near future. This low encryption does not prevent State led cracking efforts but does prevent considerable inconvenience to conventional attempts. This added to the fact that the signal is digital and skips frequency prevents all but the most sophisticated eavesdroppers to follow the signal and make copies. If you then combine this reasonable level of security to be combined with three layer authentications (username, password and daily change auth word) you have a method of connection that provides a short and medium term solution to using commercially available products for Intelligence use.

Primary issues are Telco eavesdropping (They manage the wireless link) and direct attacks on the Penokio: Couloir servers. Three layers of dual redundant Nokia carrier-grade firewalls running Checkpoint software protect Penokio. These are backed up by two NetRanger intrusion detection devices (each with fail-over). This provides a protective layer in front of Penokio: Couloir that meets the demands of all but the most determined and dedicated State sponsored hacking attempts.

Penokio: Couloir will be manned 24x7 by intrusion specialists who monitor for attempts at unauthorized access and take the necessary actions (ban access or report to agencies) including investigation of attempts. In the event of a attack, the service can be manually shut down while corrective measures can be implemented (Arrest or detention of trespassers).

The User is identified at this time (We can also implement Phone # Identification but this prevents use of a hastily obtained device which merits contingency planning).

The Penokio: Couloir Layer

Security: The Penokio layer takes the authorization information and confirms with the Oracle database that the user is authorized/denied access to information (by level, information source and depth of access). This information then unlocks the access to the Nokia VPN CC205 hardware which maintains a high encryption connection (128 modp-

1536Bit) to the state owned data sources. The State owned data sources would have their own independent security provisions that provide the necessary capstone to the process.

Device Detection: Penokio can detect the requesting device's browser (Make, Version and Language) and can then use the information to format results and input forms to the device. This feature allows the greatest possible range of wireless devices to be used for access.

Application Engine: Penokio is able to execute complex requests thus providing the necessary "horsepower" to interact with the State owned data sources (run searches etc). This has two functions: 1) Remove the need for the wireless device to have significant storage, processor and memory and 2) Allows the State owned data sources to run at their maximum efficiency without having to downgrade security and performance. This portion of the process is run on Sun Enterprise technology and iPlanet software. Sun Microsystems's hardware and technology are the most stable, secure and robust products for creating the necessary intelligent engine for mil/intel purposes.

GRPS Related Services: As location based technology is disseminated, it Penokio: Couloir will be able to log the location of the field user (within 12 Meters) and become the basis for new services: Rescue, Fire Support, Operative tracking, Location relevant data access (eg: When in Maine, access to Maine based information services first, Federal second then International third). The GPRS function has the greatest potential to provide timely and specific support to field operative.

Administration: Requests for information can become the basis for further intelligence analysis. Tracking who makes what requests can flag the information for review by supervisory people, in addition to being able to trigger automated responses to certain types or categories of information (eg. If there is an active RFI for a particular individual and there is a desire to not disseminate the general profile, if a portion of the data is requested or input (name, date of birth, Social Ins, DL, Address etc) it can trigger a routine that alerts the organization that implemented the trigger. This will permit particular agencies to maintain control over particular operations while gaining benefit from an across the board intelligence gathering effort.

Sample Scenario:

Operative logs into Penokio from a Nokia Startac device. They input their assigned ID#, PIN and Phrase of the day (which was obtained via voice match authentication that morning). The user then selects the menu relating to State DMV and due to their location Penokio knows to default to FLA (the sate they are in). They enter the license plate and run a search. Penokio then takes the license plate request, executes a watch list scan (no agencies have flagged this particular information) and makes an entry into the users log of this request. Penokio makes a request of the Florida DMV and provides the necessary credentials. The FLA DMV replies back with a standard information blurb which

Penokio then applies the display rules to (if Startac running Phone.com V 1.3 then...). The operative then receives the results in the form of a formatted list of hyperlinks (Owner, Address, Make/Model, Outstanding).

If the Owner, Address or Lic Plate of the subject of inquiry had been flagged, the information could have been denied or permitted based on the instructions in the flagging script and the agency notified of the request.

For More Information:

Robert Gagnon, CEO
FroZen Dirt Media Corporation
rgagnon@frozendirt.com

OIPE JC11
OCT 31 2002
PATENT & TRADEMARK OFFICE

Docket No. 4135-4000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Robert A. Gagnon et al.

Group Art Unit: To be Assigned

Serial No.: 09/772,132

Examiner: To be Assigned

Filed: January 29, 2001

For: SYSTEM AND METHOD FOR WIRELESS ACCESS TO A USER'S COMPUTER

EXPRESS MAIL CERTIFICATE

Express Mail Label No.: **EV 187 553 232US**

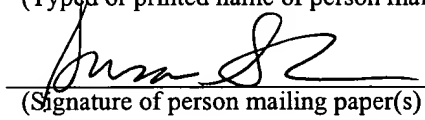
Date of Deposit: **October 31, 2002**

I hereby certify that the following attached paper(s) and/or fee

1. Petition to Make Special Under 37 CFR 1.102(d)(XI);
2. Copy of documentation from website;
3. Check of $130.00 for petition fee;
4. Return postcard

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. §1.10 on the date indicated above and is addressed to Commissioner for Patents, Washington, DC 20231

Susan Shen
(Typed or printed name of person mailing papers(s) and/or fee)



(Signature of person mailing paper(s) and/or fee)

Correspondence Address:
MORGAN & FINNEGAN, L.L.P.
345 Park Avenue
New York, NY 10154-0053
(212) 758-4800 Telephone
(212) 751-6849 Facsimile